Plaintiffs Thomas Roger White, Jr. and Christopher Mills bring this action on behalf of themselves and a class of all persons similarly situated under the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 et seq., ("CFA"), the Video Privacy Protection Act, 28 U.S.C. § 1331 ("VVPA"), the Electronic Communications Privacy Act, 18 U.S.C. § 2511 ("EECP), the Cable Privacy Act, 47 U.S.C. § 55 ("CPA"); the FTC Act, 15 U.S.C. § 45(a) (the "FTC Act"); the Subscriber Privacy Provision in the Cable Communications Policy Act, 47 U.S. Code § 551 ("CCP"); and the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 ("COPA") to obtain injunctive relief and compensation against Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. ("Samsung"); LG Electronics Inc. and LG Electronics America, Inc. ("LG"), and Sony Corporation and Sony Electronics Inc. ("Sony") (collectively, "Defendants"), and to prevent them from continuing to engage in unconscionable privacy violations, unlawful commercial practices, misrepresentations, and/or omissions of material fact in violation of the CFA, and the other statutes and laws referenced herein. In support of Plaintiffs' First Amended Class Action Complaint, Plaintiffs allege the following, based on their personal experiences and the investigation of counsel:

NATURE OF ACTION

1. Defendants are the leading manufacturers and sellers of televisions in the United States and across the world. By utilizing automatic content recognition devices/software ("ACR") and automatic recording devices/software ("ARS") that are hidden and/or installed and/or used by Defendants inside their "smart" generation of televisions ("Smart TVs"),[1] Defendants routinely – but unlawfully and secretly – (i) intercept, track and record the private communications, confidential personally-identifying data, and private watching and spending habits of consumers in their homes, and then (ii) illegally transmit that stolen information to third parties

[1] Defendants' Smart TV's are home entertainment systems that can respond to human voices and gestures.

for Defendants' commercial gain, including their reaping of hundreds of millions of dollars in advertising and other revenue.

2. But contrary to Defendants' assessment, any and all value associated with each individuals' personal, confidential data and identifying watching and spending habits, and also their own voices – (including Plaintiffs and the other members of the proposed Class) – is *not* owned by Defendants. Rather, it is the personal property of each individual consumer; it is ever-changing and evolving with the individual him- or herself. As such, Defendants' illegal "back door" theft of users' confidential data, personally-identifiable information, and their voices using high-tech encryption and outside data-processing firm - and Defendants covert sale of that sensitive information on the black market for their own financial gain, is unlawful and threatens to erode our civilized-society itself.

3. Upon information and belief, Defendants' Smart TVs are able to secretly track and record – not only the purchaser of the Smart TV – but *any person in the home*.[2]

4. Defendants accomplish their pirating of consumers' confidential information and voice recordings by employing the services of sophisticated data processors and information-recognition companies, such as Cognitive Networks, that:

> *partner[] with TV set manufacturers to enable content providers, advertisers, and others to provide greater engagement and interactivity to TV programming. Cognitive Networks' ACR (automatic content recognition) platform makes Smart TVs aware of the programming that they are displaying, enabling transactions [and] informational requests . . . .*[3]

[2] Upon information and belief, Defendants and the third parties they transmit consumer data and recordings to create a separate "f*ingerprint*" of personal-watching habits and confidential information for different individuals in a home where a Smart TV is located.

[3] See https://techcrunch.com/2015/01/04/cognitive-networks-ces/ (reiterating Cognitive Networks partnership with Defendants LG); http://www.prweb.com/releases/2012/11/prweb10185158.htm;

5. As Zeev Neumeier, Cognitive Network's Founder and President, explained, third-party data-recognition companies that Defendants employ to collect private confidential information, watching and spending habits, and voice recordings about consumer utilize ACR technology that:

> *[L]ooks at the picture on your TV and uses that data to identify exactly what you're watching. That, in turn, enables a content provider or advertiser to add interactive overlays to the TV screen itself, triggered by what's onscreen at the moment — say, a poll that's relevant to a scene in a show or a coupon that's tied to an ad.*[4]

6. Defendants' Smart TVs also routinely and secretly intercept and record the private communications of consumers in their homed by utilizing additional automatic recording software ("ARS") that they conceal inside and/or use with their Smart TVs [hereinafter, Defendants' combined ACR and ARS technology will be referred to herein as "*Automatic Content Software*" or collectively as "*ACS*"].

7. Having unlawfully acquired personally-identifying, confidential information and private conversations about consumers through Defendants' ACS (including information that identifies a person as having obtained or requested specific video materials or services), upon information and belief, Defendants then transmit this confidential personally-identifying information and private conversations to third parties and data processors/brokers for profit, in violation of, amongst other laws, the CFA, the VVPA, the EECP, the CPA, the FTC Act, the CCP, and the COPA, and various other statutes and laws. [5] See infra.

---

https://www.crunchbase.com/organization/cognitive-networks. See also **(Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 1).**

[4] https://techcrunch.com/2015/01/04/cognitive-networks-ces/. See also See also (Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 1).

[5] Defendants' Automatic Content Software also routinely and secretly intercept and record the private communications of consumers in their homes – including children's voices in violation of the Children's Online Privacy Act) (the "COPA"). See infra.

8. Unbelievably, Defendants even use their Automatic Content Software, upon information and belief, to push targeted ads to consumers, even on the ***other*** separate-unrelated electronic devices that share the same internet network-connection as a Defendants' Smart TVs. That is, for instance, under Defendants' set up, a person watching a "romantic television program" on Defendants' Smart TV in the privacy of their home may then receive advertisements for sexy lingerie on their non-related, separate telephone – even later in time in the workplace.[6]

9. Furthermore, Defendants' representations were not sufficiently clear or prominent to alert consumers to their practices related to their tracking, recording, and personal-data collection, and transmission of consumers' private information and voices to third parties, for profit. Consumers, including Plaintiffs and the Class, have no reason to expect that Defendants engage in second-by-second tracking of consumer viewing data and recording of spoken words by surreptitiously decoding content and sending it back to their own servers and/or to the servers of third parties, for profit. In addition, the separate privacy policies of the third parties that Defendants transmit private consumer-data and recording to were never disclosed to Plaintiffs and/or the proposed Class members. Thus, for the vast majority of consumers who are unaware of the need to take steps to ensure their privacy, Defendants do nothing to alert them, preferring to keep their invasive monitoring, tracking, and recording practices – their "backdoor billion-dollar business" – a secret from its customers.

10. To the extent that any words transmitted to Plaintiffs and the Class are to be construed in any way to form a contract, such agreement would be deemed a classic Contract of Adhesion under common law, without informed consent, and thus unenforceable as a matter of law.

[6] During its investigation, this exact scenario has been reported by several individuals to Counsel for Plaintiffs and the proposed Class.

11. Plaintiffs and the proposed Class Members did not know about and did not consent to Defendants' placement and/or use of Automatic Content Software inside the Smart TVs they purchased, and/or Defendants' tracking and/or recording of Plaintiffs and the Class via Defendants' Smart TVs, and/or Defendants transmission of private consumer information and voices to third parties, and/or Defendants transmission of private consumer information and voices to third parties for profit. Had they known about Defendants' false, deceptive, unfair, and misleading course of conduct, described herein, Plaintiffs and the Class members would not have purchased Defendants' Smart TVs or, at a minimum, would have purchased fewer products and/or paid less for the products they did purchase.

12. Defendants also recklessly and/or negligently failed to use reasonable care to protect the private recordings and personally-identifying information that they steal from consumers. Upon information and belief, some private communications and data that Defendants' take from unsuspecting consumers are transmitted by Defendants to third parties without proper encryption, which has allowed outside third parties to hack and gain access to Plaintiffs and the Class' private recordings and information (causing further harm to Plaintiffs and the Class). See infra.

13. In fact, wholly inadequate protections regarding Smart TV-"hidden spying systems" was revealed publicly on March 7, 2017, when WikiLeaks reported that Smart TVs were in fact being used by outside parties to spy on consumers' private-conversations, *even when the device was supposedly turned "off."*

14. Defendants' actions are an unconscionable commercial practice in violation of the CFA and the other federal statutes and laws referenced herein. Each separate instance of Defendants' recording, tracking, storing, and/or transmitting personal data and/or information, including watching habits, of consumers

constitutes a separate violation under the CFA, subjecting Defendants to separate penalties and violations for each instance of misconduct. N.J. Stat. Ann. § 56:8-2.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §1332(d)(2), because the proposed class has more than 100 members, the class contains at least one member of diverse citizenship from Defendants, and the amount in controversy exceeds $5 Million.

16. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because certain claims arise under federal law, namely the CFA, the VVPA, the EECP, the CPA, the FTC Act, the CCP, and the COPA, This Court has supplemental jurisdiction over state law claims.

17. The Court has personal jurisdiction over Defendants because Defendants are headquartered and/or have corporate offices in the state of New Jersey and Defendants regularly transact business within the State of New Jersey. Moreover, the deceptive and misleading sales, advertising and marketing of Defendants' products in the United States in substantial part originates in and emanates from New Jersey.

18. Venue properly lies in this District pursuant to 28 U.S.C. §1391(a)(1), because Defendant Samsung is headquartered and conducts its business from 105 Challenger Road, Ridgefield Park, NK 07660, which is in this District; Defendant LG is headquartered and conducts its business from located at 1000 Sylvan Avenue Englewood Cliffs, New Jersey, U.S.A. 07632, which is in this District; and Defendant Sony maintains its corporate campus and conducts substantial business in New Jersey in this District, including at its corporate office at Sony Drive, Park Ridge, NJ 07656. Venue also properly lies in this District because all Defendants

conduct substantial business within this District, and because many of the Class Members reside in this district.

Application of New Jersey Law To
Consumers Nationwide is Appropriate

19. Each of the defendants are headquartered and/or have a substantial corporate presence in New Jersey and, upon information and belief, Defendants' United States sales strategy, advertising, marketing and product promotion was conceived in substantial part, and emanates from, Defendants' facilities in New Jersey.

20. Application of New Jersey law to consumers nationwide is appropriate because Defendants are headquartered here and/or maintain their US based corporate, marketing and advertising department(s) in New Jersey where the alleged misconduct, described herein, emanated from. In addition, upon information and belief, Defendants' products are distributed throughout the United States to Plaintiffs and Class members located in New Jersey and/or distributed throughout the United States from facilities located in New Jersey. New Jersey also has a substantial, compelling reason to protect consumers from deceptive and unlawful misconduct of companies with headquarters and a substantial presence there, and who regularly sell products in and/or from New Jersey.

THE PARTIES

21. Plaintiff Thomas Roger White, Jr. is a resident and citizen of Miami Shores, Florida. During the Class Period, Mr. White purchased two Samsung Smart TVs, one Sony Smart TV, and one LG Smart TV, which are the subject of this dispute. At all times during the Class Period, Mr. White was unaware, amongst other things, that: (i) Defendants' Smart TVs collect personally identifying information, including information that identifies a person as having obtained or requested

specific video materials or services; or (ii) Defendants' Smart TVs contain and/or use Automatic Content Software; or (iii) Defendants secretly transmit private, confidential information and voices of consumers to third parties, such as advertisers and data brokers (who store that information on their servers); or (iv) that Defendants had made inadequate disclosures to Plaintiffs and the Class members regarding Defendants' Automatic Content Software and use and sale of that data and information for profit.

22. Plaintiff Christopher Mills is a resident and citizen of New York, New York. During the Class Period, Mr. Mills purchased a Samsung Smart TV which is the subject of this dispute. At all times during the Class Period, Mr. Mills was unaware, amongst other things, that: (i) Defendants' Smart TVs collect personally identifying information, including information that identifies a person as having obtained or requested specific video materials or services; or (ii) Defendants' Smart TVs contain and/or use Automatic Content Software; or (iii) Defendants secretly transmit private, confidential information and voices of consumers to third parties, such as advertisers and data brokers (who store that information on their servers); or (iv) that Defendants had made inadequate disclosures to Plaintiffs and the Class members regarding Defendants' Automatic Content Software and use and sale of that data and information for profit.

23. Defendant Samsung Electronics America, Inc. is headquartered at 105 Challenger Road Ridgefield Park, N.J. 07660, conducts substantial business in New Jersey, and is a subsidiary of Defendant Samsung Electronics Co., Ltd., a Republic of Korea limited company with its principal place of business in 250, 2-gaaepyong-ro, Jung-gu, Seoul 100-742, Korea. Samsung is the market leader for HDTVs in the U.S.

24. Defendant LG Electronics USA, Inc., is headquartered at 1000 Sylvan Avenue Englewood Cliffs, New Jersey, U.S.A. 07632, conducts substantial business

in New Jersey, and is the North American subsidiary of Defendant LG Electronics, Inc., a $48.5-billion global force in consumer electronics, home appliances and mobile communications.

25. Defendant Sony Corporation is a Japanese multinational conglomerate corporation that is headquartered in Kōnan, Minato, Tokyo. Defendant Sony Electronics Inc. is a subsidiary of Sony Corporation, conducts substantial business in New Jersey and maintains its corporate campus at Sony Drive, Park Ridge, NJ 07656.

N.J. STAT ANN. § 56:8-2

26. The CFA, N.J. Stat. Ann. § 56:8-2, prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . .

27. The CFA defines "merchandise" as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." N.J. Stat. Ann. § 56:8-1(c).

28. Defendants have engaged in the advertisement, offering for sale and sale of merchandise within the meaning of N.J. Stat. Ann. § 56:8-1(c); specifically Defendants' Smart TVs and related products and services.

BACKGROUND

Congress Anticipated the Privacy Threats of "Interactive Television" In the Early 1980s

29. Concerns about the use of televisions to collect consumer information were anticipated in the 1980s.[7]

30. Privacy scholars and policy makers recognized the risk that interactive television would threaten the privacy of users if safeguards were not established.[8]

31. These risks included the "danger similar to wiretapping," of "misuse and interception of 'private' information" during transmission to the central servers, as well as the insecurity of data once it arrived at the central servers.[9]

32. The Cable Communications Policy Act (the "Cable Act") was enacted in 1984 to combat these risks.[10]

33. The Cable Act ensures, amongst other things, that cable operators collect only the user data needed to operate the service, keep the data secure while it is in use, and delete the data once it has served its purpose. It also gives cable consumers the right of access to their data.[11]

34. According to the Senate Committee on Commerce, Science, and Transportation, "the development of new and diversified services over interactive two-way cable systems should not impact adversely upon the privacy of the individual."[12]

---

[7] 11 David A. Bode, Interactive Cable Television: Privacy Legislation, 19 Gonz. L. Rev. 725 (1984).
[8] See William J. Broad, U.S. Counts on Computer Edge in Race for Advanced TV, N.Y. Times (Nov. 28, 1989), http://www.nytimes.com/1989/11/28/science/us-counts-o-computer-edge-in-the-race-for-advancedtv.html ("Finally, scientists say, the advent of digital television will aid the merging of computers and television, with the prospect of a rush of combined uses."); David Flaherty, Protecting Privacy in Two Way Electronic Services, Communications Library (1985).
[9] Bode, supra 13 at 711. See also *Cable Television Privacy Act: Protecting Privacy Interests from Emerging Cable TV Technology*, 35 Fed. Com. L.J. 71, 79 (1983).
[10] Cable Communications Policy Act of 1984, 47 U.S.C. §§ 601-639. 16 Id at §631. 17 S.Rep. No. 67, 98th Cong., 1st Sess. 27 (1983).
[11] Id.
[12] S.Rep. No. 67, 98th Cong., 1st Sess. 27 (1983).

35. The FTC Chair has addressed the specific problem of consumer devices that spy on consumers. Chair Ramirez stated, "Reasonable limits on data collection and data retention is the first line of defense for consumer privacy."[13]

FACTS

36. Defendants bill themselves as leading high definition television producers in the United States. In addition to Smart Televisions ("Smart TVs"), Defendants manufacture and sell various audio and entertainment products. Defendants generated billions in revenue in 2016.

37. In or around January 2012, Defendants' began selling Smart TVs. Defendants' Smart TVs provide consumers with multiple access points to visual, audio, and other video content. Defendants' Smart TVs are equipped with HDMI connections, coaxial connectors, analog audio outputs and inputs, and various video input connectors.

38. Defendants' Smart TVs are also equipped with the ability to connect to the internet via wireless internet networking (hereinafter "WiFi"). Specifically, Defendants' Smart TVs allow consumers to access the WiFi networks to allow consumers to access and watch various forms of audio and visual entertainment online, as well as to find access to online news, weather, and entertainment sources.

39. Defendants' Smart TVs are delivered to consumers with many pre-installed applications. These include such popular internet applications as Netflix, YouTube, Amazon, Pandora, HuluPlus, Twitter, and more. The list is ever-growing. Many of these applications stream video and other content to consumers via Defendants' Smart TVs.

40. Additionally, Defendants' Smart TVs provide access to cable television, satellite television, and on-demand viewing services. Such services also stream video and audio programming directly to Defendants' Smart TVs.

[13] http://www.usnews.com/news/articles/2015/01/06/the-internet-of-things-ftcchairwoman-calls-for-tech-privacy-at-ces

41. Upon information and belief, since 2012, Defendants have manufactured Smart TVs that continuously monitor and track, in real time, what consumers are watching and the viewing habits of those consumers, and also record the voices of consumers, and then transmit that private, confidential information to Defendants' own servers by means of proprietary, Automatic Content Software ("ACS").[14]

42. Defendants' ACS enables Defendants to monitor and identify Plaintiffs' and the Class Members' video viewing habits and voices. Defendants' then, upon information and belief, secretly provide this private, sensitive information and voices of consumers to third-party advertisers and content providers who, in turn, display targeted advertisements to consumers, based on this sensitive personal information and voice recordings. In addition, upon information and belief, Defendants even place advertisements, based on consumers' data and information they have secretly acquired from their ACS, within some Smart TV apps in the Smart TVs themselves.

43. For instance, Defendant Samsung has identified a company called "Nuance" as third party it transmits consumers' information to[15] and also has identified a company called "Enswers" as a third party it transmit consumers'

[14] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm; The Verge, *Most smart TVs are tracking you – Vizio just got caught,* February 7, 2017, http://www.theverge.com/2017/2/7/14527360/vizio-smart-tv-tracking-settlement-disable-settings.

[15] Id. Samsung has identified the third party as Nuance, a voice-to-text recognition company it utilizes. *Samsung Tomorrow, Samsung Smart TVs Do Not Monitor Living Room Conversations* (Feb. 10, 2015), http://global.samsungtomorrow.com/samsung-smart-tvs-do-not-monitor-living-room-conversations/.

information to; and Defendant LG has identified Cognitive Networks[16] as a third party it transmit consumers' information to.[17]

44. As a Consumer Report investigation uncovered:

> Here's how it works: Companies such as Cognitive Networks, Enswers, and Gracenote collaborate with television manufacturers to embed [automatic tracking software] technology into smart TVs that monitors either the voice or audio stream – and sometimes both – that the user is watching. The [automatic tracking software] creates a "fingerprint" of the on-screen content, and then send it to a remote server that uses that fingerprint to determine what programming is being watched. Since much of the [automatic tracking software] process is handled by these third parties, *it is likely that millions of smart TV owners have inadvertently left an extensive data trail chronicling months, if not years, of their TV-watching history on the servers of companies they have never heard of*.[18]

---

[16] Defendants accomplish their pirating of consumers' confidential information and voice recordings by employing the services of sophisticated data processors and information-recognition companies, such as Cognitive Networks, that:

> partner[] with TV set manufacturers to enable content providers, advertisers, and others to provide greater engagement and interactivity to TV programming. Cognitive Networks' ACR (automatic content recognition) platform makes Smart TVs aware of the programming that they are displaying, enabling transactions [and] informational requests . . . .

See https://techcrunch.com/2015/01/04/cognitive-networks-ces/ (reiterating Cognitive Networks partnership with Defendants LG); http://www.prweb.com/releases/2012/11/prweb10185158.htm; https://www.crunchbase.com/organization/cognitive-networks. See also (Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 1).

[17] "Sony TVs today use Android TV, which means you're subject to Google's data-collection practices as well." See Techworm, *Android smart TVs can be hacked to spy on your conversation*, May 17, 2016, https://www.techworm.net/2016/05/hackers-can-spy-say-hacking-sony-made-android-tvs.html (Reporting that hackers can easily obtain your private information by hacking Sony made Android TVs).

[18] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm (emphasis added).

45. Cognitive Networks has admitted using consumer information it has obtained from Defendants for advertising purposes. In a 2013 press release, the company highlighted the value of ACS for advertisers, who could not otherwise "pinpoint what viewer's interests are and provide more targeted advertisements based on their preferences." In fact the market research firm for Cognitive Networks lists the "always on" nature of ACS as one of its key benefits, and claims: "The consumer does not need to opt-in to an app or service in order to interact with enhanced TV features."[19]

46. As Zeev Neumeier, Cognitive Network's Founder and President, explained, the data recognition/processor, third-party companies like Cognitive Networks that Defendants employ to collect private confidential information and watching habits about consumer utilize:

> *[A]utomatic content recognition (ACR) that looks at the picture on your TV and uses that data to identify exactly what you're watching. That, in turn, enables a content provider or advertiser to add interactive overlays to the TV screen itself, triggered by what's onscreen at the moment — say, a poll that's relevant to a scene in a show or a coupon that's tied to an ad.*[20]

47. Enswers has admitted that, in 2012, its tracking software has been embedded at the hardware level into Samsung smart TVs. Enswers has already used the technology to push interactive advertisements for retirement-planning financial products in Spain, and also has prompted Samsung smart TV owners to purchase David Beckham underwear during the Super Bowl XLVIII using their remote controls.[21]

---

[19] Id. at 1. See also (Cognitive Network's Automatic Content Software Platform Diagram) (attached hereto as Exhibit 1).

[20] https://techcrunch.com/2015/01/04/cognitive-networks-ces/. See also Id.

[21] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm

48. Through Defendants' ACS, their Smart TVs are able, upon information and belief, to transmit information about what a consumer is watching on a second-by-second basis, in addition to the voices of users. Upon information and belief, Defendants' tracking software captures information about a selection of pixels on the screen and sends that data to Defendants' servers, where it is uniquely matched to a database of publicly available television, movie, and commercial content. Defendants collect viewing data from cable or broadband service providers, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts. Upon information and belief, Defendants store this data indefinitely.

49. Defendants' ACS software also periodically collects other information about the television, including IP address, wired and wireless MAC addresses, WiFi signal strength, nearby WiFi access points, and other items.

50. Upon information and belief, Defendants earn substantial revenue by providing consumers' television viewing history to third parties through licensing agreements, on a television-by-television basis.[22]

51. Upon information and belief, Defendants have provided consumers' data, voices and sensitive information to third parties for the purpose of targeting advertising to particular consumers on their other digital devices based on their television viewing data.

52. Defendants also facilitate the provision of demographic information to third parties about Defendants' television viewers. Upon information and belief, Defendants do this by providing consumers' IP addresses to a data aggregator. The data aggregator uses the IP address information to identify a particular consumer or household, and then sends third parties the demographic information associated with

[22] Precise data about consumers TV viewing habits is big business. Revenues for audience-measurement company Nielsen surpassed $6 Billion last year. Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch, Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm

that consumer or household. Upon information and belief, Defendants' contracts with third-party users of the viewing data allow the following information to be appended: sex, age, income, marital status, household size, education, home ownership, and household value. For all of these uses, Defendants provide highly-specific, second-by-second information about television viewing.

53. Defendants' ACS tracking software works by analyzing bits of the video and other visual programming its customers are watching, in real time. The technology then allows Defendants' to determine, amongst other information, the date, time, channel of programs, and whether customers watched this programming in real time or from a recording.

54. Upon information and belief, Defendants' ACS tracking technology also allows Defendants to determine whether a viewer is watching a traditional television or cable program or whether the customer is viewing programming via streaming internet applications such as Netflix, Amazon Prime, or Hulu. The technology determines the time frame during which the programming was viewed, as well as the duration for which the customer actually viewed it.

55. Defendants, armed with this surreptitiously-collected information on customers' viewing habits, then connect the information to the customers' personal internet protocol (hereinafter "IP") address. This is the internet address that is used to identify every internet connected device in a home, office, or other connected environment. These devices include smartphones, tablet computers, laptop computers, desktop computers, and any other wireless device that shares the same IP address as the Smart TV.

56. IP addresses are closely connected to the individuals using the specific IP address. For instance, hundreds of personal attributes can be connected to a specific IP address, including a customers' age, profession, and certain wealth indicators.

57. Upon information and belief, Defendants' ACS is also designed to scan a consumer's home WiFi networks to secretly collect information that is then utilized to help determine the specific person whose viewing activity has been collected.

58. To accomplish this, upon information and belief, Defendants' provide the collected information to databrokers, which are entities that offer data enhancement services. These brokers are able to match the information to information in its database. Linking the two datasets allows the data broker to inform Defendants, and thus, indirectly, Defendants' third-party customers, of the identity of the individual watching the specific programming on Defendants' Smart TV. That is, upon information and belief, Defendants' ACS actually allows Defendants to determine, within a certain degree of accuracy, which person in a home is watching what and when.

59. Armed with this secretly-collected viewing information, upon information and belief, Defendants then sell consumer private information to third parties, including advertisers. Doing so allows advertisers and marketers to determine which advertisements to display on not only a consumer's Defendants' Smart TV, but also any other "smart" devices connected to the same IP address, such as smartphones, tablets, and computers. Accordingly, upon information and belief, watching a specific program on the Defendants' Smart TV allows advertisers to determine which advertisements to publish on your smartphone.

60. In other words, Defendants are secretly spying on its customers for profit. Defendants do not deny that they are violating its customers' privacy in this manner.

61. Consumers have no reason to expect that Defendants engaged in second-by-second tracking of consumer viewing data by surreptitiously decoding content and sending it back to their own servers, and then on to third parties' servers.

Further, Defendants' representations were not sufficiently clear or prominent to alert consumers to their practices related to data collection and transmission.

62. Defendants' Smart TV set up does not specifically state that Defendants monitor, track, and report viewing habits and private information about devices attached to home networks, or that Defendants then transmit that information to third parties for profit. Nor do Defendants' proactively notify its consumers that the company will be collecting the consumers' viewing data by utilizing the pre-installed tracking software or the specific third-parties Defendants have contracts with. Rather, Defendants omit this material information in its communications with its consumers.

63. In reality, Defendants conceal their ACS and the method for disabling it. In order to not be subjected to Defendants ACS and monitoring programs forever, the consumer must somehow – while taking the unit out of a cardboard box and attempting to physically install it (or, as is often the case, having someone else set it up for the consumer):

a. find the privacy policy, read and comprehend the complex legal text;

b. understand how, why, when, and if Defendants are collecting confidential information about them;

c. determine whether or not Defendants' data collection is for Defendants' profit;

d. figure out if Defendants are monitoring and collecting their personal information in real time;

e. try to compute how much information Defendants are collecting and from which devices; and

f. determine if Defendants are storing consumers' private information on their servers, and for how long.

64. Then, consumers must figure out:

i. when and if Defendants are transmitting their information to outside third parties,

ii. how much information they are transmitting to third parties and for what purposes,

iii. to what third parties they are transmitting consumer information to, and what the privacy policies of the outside third parties are; and

iv. whether the third parties are storing consumers' private information on their servers, and for how long.

65. Consumers must further figure out:

a. if those outside third parties are transmitting their personal information to other outside "second level" third parties, and

b. to what "second level" third parties Defendants are transmitting consumer information to;

c. how much information they are transmitting to "second level" third parties and for what purposes;

d. what the privacy policies of the outside "second level" third parties are; and

e. whether the "second level" third parties are storing consumers' private information on their servers, and for how long.

66. As a Consumer Reports investigation about Defendants' Smart TVs determined:

> [A] key concern with the user monitoring features now built into smart TVs: Consumers don't know precisely what they're enabling when they click through the TV's privacy policy. When Consumer Reports set up a current Samsung smart TV, we were confronted with a terms of service and privacy agreement that had *nine separate expandable sections to explore*. One section, the "Smart Hub Privacy Policy," *covered 47 screens' worth of text*. Users setting up an LG set will see terms of use with *18 sections and a privacy policy with 11 separate sections, and a rider screen asking them to*

> *okay three additional services*—**in total, more than 6,000 words of legal disclosure.** Regardless, both [LG and Samsung Smart] TVs allow you to zip through these agreements by agreeing to them all at once. *And a consumer could hardly be blamed for not wanting to read thousands of words of legal documentation on their TVs when they're trying to set them up for the first time*.[23]

67. Furthermore, Defendants' customers do not have access to the names of the outside third parties (or outside "second level" third parties) or access to the separate privacy policies of these outside parties (or outside "second level" third parties) or access to the licensing agreements between Defendants and these third parties. Thus, for the vast majority of consumers who are unaware of the need to take steps to ensure their privacy, Defendants do nothing to alert them, preferring to keep their invasive monitoring and tracking practices – their "backdoor billion dollar business" -- a secret from its customers.

68. Further, even were a consumer to understand the privacy policy and the so called "option" to not be subjected to Defendants ACS and automatic monitoring programs, upon information and belief, consumers are then unable to use some or most of the "Smart" features on their Smart TV -- the very reason consumers buy (and pay considerable extra) when purchasing Smart TVs in the first place.[24]

---

[23] See Consumer Reports, *Samsung, LG, and Vizio smart TVs are recording—and sharing data about—everything you watch*, *Consumer Reports investigates the information brokers who want to turn your viewing habits into cash*, February 27, 2015, http://www.consumerreports.org/cro/news/2015/02/samsung-lg-vizio-smart-tvs-watch-everything-you-watch/index.htm.

[24] See, e.g. TechDirt, *LG Will Take The Smart Out Of Your Smart TV If You Don't Agree To Share Your Viewing and Search Data With Third Parties*, May 20,2014, https://www.techdirt.com/articles/20140511/17430627199/lg-will-take-smart-out-your-smart-tv-if-you-dont-agree-to-share-your-viewing-search-data-with-third-parties.shtml; See also Slashdot, *Television Privacy Declining LG's New Ad-friendly Privacy Policy Removes Features From Smart TVs* ("Techdirt and Consumerist posted articles about a user . . . [who] declined their new [LG Smart TV] Privacy Policy, only to find that most Internet-connected features (e.g. BBC iPlayer, Skype) of the TV now no longer work."), May 21, 2014, https://entertainment.slashdot.org/story/14/05/21/1456206/declining-lgs-new-ad-friendly-privacy-policy-removes-features-from-smart-tvs.

69. Further, upon information and belief, Defendants' Smart TVs have continued to collect private information about consumers' even when consumers have successfully "opted out" of such monitoring.[25]

Defendants Sells Smart TVs that Record
Voice Communications in the United States

70. Beginning in 2012, Defendants developed techniques to monitor and recognize voice communications.

71. The first such Smart TV was announced at the Consumer Electronic Expo in 2012.[26]

72. Defendants' remote controls have either a built-in microphone for voice recognition; some other Smart TV models include a camera and additional microphones to recognize voice and hand gesture.[27]

73. As of 2015, Smart TVs sales reached almost 200 million units. Sales are expected to grow to 330 million by 2019.

74. Upon information and belief, when the voice recognition feature in Defendants' Smart TV is used (which is the "selling feature" of Defendants' Smart TV -voice recognition – televisions), unbeknownst to consumers, everything a user says in front of Defendants' Smart TVs is recorded by Defendants and transmitted over the internet to a third party regardless of whether it is related to the provision of the service.[28]

---

[25] See, e.g., NetworkWorld, *LG Smart TV spying, owner claims his USB filenames posted on LG servers*, Nov. 19, 2013, http://www.networkworld.com/article/2225848/microsoft-subnet/lg-smart-tv-spying--owner-claims-his-usb-filenames-posted-on-lg-servers.html.

[26] See Christina Bonnington, Samsung Smart TV 2.0 Can 'Liste See and Do', Wired (Jan. 9, 2012), http://www.wired.com/2012/01/samsung-smart-tvs-ultrabooks/

[27] See Casey Johnston, Hands-on: Gesture, Voice, and the Many Inputs of Samsung's Smart TV, ArsTechnica (Mar. 6, 2012), http://arstechnica.com/gadgets/2012/03/hands-on-gesture-voice-and-themany-inputs-of-samsungs-smart-tv/.

[28] See, e.g., In re: Samsung Electronics Co., Ltd. 20 Federal Trade Commission, February 24, 2015 at 13 (the "FTC Brief") (attached hereto as Exhibit 2).

75. As described herein, Consumers have no reason to expect that Defendants engaged in second-by-second tracking and recording by surreptitiously recording content and sending it back to their own servers and then transmitting that information to third parties. Further, Defendants' representations were not sufficiently clear or prominent to alert consumers to their practices related to Defendants' recording of consumers' private recordings in their home.

Defendants' Practices Violate the Subscriber Privacy Provision in the Cable Act

76. The Subscriber Privacy Provision in the Cable Communications Policy Act ("CCPA") prohibits the collection of "personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned."[29]

77. The CCPA also provides, "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[30]

Defendants' Practices Violate the Subscriber Privacy Provision in the Cable Act and the FTC Act

78. The Subscriber Privacy Provision in the Cable Communications Policy Act ("CCPA") prohibits the collection of "personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned."[31]

[29] 47 U.S.C. § 631(b).
[30] Id.
[31] 47 U.S.C. § 631(b).

79. The CCPA also provides, "a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator."[32]

80. Defendants do not obtain written or electronic consent to their use of ACSs to collect and transmit consumers' private, confidential information and watching habits to third parties.

81. Defendants do not "take such actions as are necessary to prevent unauthorized access" to subscriber information and, in fact, Defendants deliberately overcollect information provided by cable subscribers, in contravention to Congress' explicit purpose for passing the subscriber privacy section of the CCPA.[33]

82. Upon information and belief, Defendants do not obtain valid written or electronic consent to recording the private conversations of people in their homes and transmitting those voice recordings to third parties for profit.

83. Upon information and belief, Defendants not "take such actions as are necessary to prevent unauthorized access" to subscriber information.

84. In fact, Defendants deliberately overcollect information provided by cable subscribers, in contravention to Congress' explicit purpose for passing the subscriber privacy section of the CCPA. See, supra.

85. Defendants are violating the CCPA.[34]

86. Defendants' misconduct described herein also violates the FTC Act, 15 U.S.C. § 45(a) (the "FTC Act"). The FTC Act prohibits "unfair or deceptive acts or unfair practices in or affecting commerce." Misrepresentations or deceptive omissions of material fact constitute deceptive acts or unfair practices prohibited by

[32] Id.
[33] Id.
[34] Id.

Section 5(a) of the FTC Act. Business practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

Defendants' Business Practices Violate Children's Online Privacy Protection Act

87. Defendants market Smart televisions to children under the age of 13. In fact, Samsung publicly concedes this fact.[35]

88. As described above, Defendants routinely record conversation in the home, including children's voices, and transmits these conversations to third parties.

89. By failing to ask parents' permission to record, store, and transmit children's voices to a third party, Defendants fail to "[p]rovide a reasonable means for a parent to review the personal information collected from a child and to refuse to permit its further use or maintenance."[36]

90. Parents cannot reasonably review the personal information that, upon information and belief, Defendants collect from children in the course of recording users' private conversations in the home.

91. Therefore, Defendants failures to obtain parental consent for the collection and transmission of children's voices constitutes violations of the Children's Online Privacy Protection Act, 16 C.F.R. § 312.3 (2013).

[35] Samsung specifically targets some features of the SmartTV to young children. The Hopster Smart TV App "brings preschoolers an extensive catalogue of hundreds of episodes of award-winning TV shows." Samsung, Samsung Partners with Hopster to Bring TV and Learning Platform for Children to Smart TV (Dec. 10, 2014), http://www.samsung.com/uk/news/local/samsung-partners-with-hopster-to-bring-tv-andlearning-platform-for-children-to-smart-tv. Id. ("The addition of Hopster to the Samsung Smart Hub means that families can now enjoy even more great content together at home").

[36] FTC Samsung Brief at 19.

Consumers Do Not Believe That Defendants' Voice Recognition Involves Voice Recording or Transmission

92. The Electronic Privacy Information Center ("EPIC"), a leading consumer group before the FTC[37], has compiled many statements from consumers regarding the fact that they never knew (or could possibly imagine) that voice recognition system in Smart TVs could intercept and record private communications in the home, or that Defendants would transmit those private recordings to outside parties.[38]

93. For example, a Smart TV user Dane Jensen commented:

> This is an outrageous invasion of privacy and should be illegal. Actually it is illegal but not being enforced. You are not allowed to spy or record someone without consent. I just bought a Samsung TV and never saw or signed any consent form to be recorded. I never saw anything.[39]

94. User Stephen commented:

> This should have to be relayed to the customer prior to purchasing. Shame on Samsung for giving into the governments constant strive to monitor the entire population[40]

95. User potrzebie commented, "I own two Samsung TVs and a Samsung tablet. If they don't stop this right now, I will never buy another Samsung product, ever. Vote with your wallets people.[41]

---

[37] See In re: Samsung Electronics Co., Ltd. 20 Federal Trade Commission, February 24, 2015 (the "FTC Samsung Brief") (attached hereto as Exhibit 2). EPIC has already deemed Defendants conduct alleged herein to be misleading and deceptive, and has argued to the FTC that "Samsung users could not reasonably have anticipated that by using a voice-controlled Smart TV, their private conversations would be transmitted, sometimes unencrypted, to a third party company." Id. at 19.

[38] The survey conducted by EPIC only concerned Samsung Smart TV users, but the confusion expressed there applies equally to all Defendants. Counsel for Plaintiffs is more than willing to perform similar surveys for each Defendant if the Court so desires.

[39] Id. at 7.

[40] Id.

[41] Id.

96. Twitter user @Jason_Garber commented, "From now on wherever I have business meetings and there is a #Samsung #SmartTV present I will ask for its removal."[42]

97. Twitter user @CSElder commented, "@Samsungtweets i will NEVER buy another Samsung tv thanks to your recording feature. You overstep your bounds. #SamsungFail"[43]

98. User beverly commented, "why is this info sent to third party at all it should just stop at the smart tv processor" [44]

99. User cft6vgy7 commented,

> This is why devices like cameras and microphones should always be sold separately from computers, TVs, and other electronics. It may not be as "convenient" for the less tech-savvy, but it will be more secure for every single consumer. Allow consumers to "opt-in" if they don't mind the security risk; don't force users to have to "opt-out" if they want to preserve their own privacy. [45]

100. User John Manso wrote,

> I'm glad this is getting national attention. When I first saw the smart TV's come out, very few were concerned. A device in your living room with a camera, a microphone, and 24 hour access to the internet. What could go wrong here? Uh, everything. Who knows who can hack into all of these with a simple piece of software. Everything can be "hacked". No we don't cook up national threats in our living room but privacy is expected and deserved in one's living room wouldn't you say?[46]

101. User Craig Cheatham commented:

---

[42] Id.
[43] Id.
[44] Id.
[45] Id. at 7-8.
[46] Id. at 8.

> There are a couple problems evident here beside the obvious one of spying on our conversations. All of these User Agreements convey all sorts of rights to the company without articulating them in a clear manner to the consumer. . . . There is NO way to know what is "shared" or who has access to it. . . . This trope of Future Shock is a new societal psychological syndrome, as yet unnamed. It is not really paranoia, it is a response to the unwilling sharing of our personal lives that we are powerless to stop without becoming a tree dwelling Luddite. It is an intrusion into what had been considered private personal space.[47]

Facts Related To Plaintiffs

102. Plaintiff Thomas Roger White, Jr. caused to be purchased during the Class Period a LG Smart TV, a Sony Smart TV, and two Samsung Smart TVs for use in his home in Miami Shores, Florida. Plaintiff Espinoza caused to be purchased during the Class Period a Sony Smart TV for use in his home in Kennesaw, Georgia. Plaintiff Christopher Mills caused to be purchased during the Class Period a Samsung Smart TV for use in his home in New York, New York.

103. Each Plaintiff, since the purchase of Defendants' Smart TVs connected their Smart TV to the internet via their home wireless network and watched shows, movies, and other entertainment programs, often through pre-loaded applications on the Smart TV.

104. Plaintiffs did not consent at the time of purchase and set-up, nor have they consented at any time since, to the operation of Defendants' automatic tracking software on their Smart TVs. Additionally, Defendants did not adequately notify Plaintiffs of Defendants' use and/or pre-installation of automatic tracking software, and/or that Defendants were actively monitoring their viewing habits, either in printed materials contained in the Smart TV packaging or in the prompts guiding Plaintiffs through the setup of the Smart TV.

[47] Id.

105. Had Plaintiffs known that Defendants installed and/or used automatic tracking software on their television sets and that they were actively monitoring their viewing habits, and/or that Defendants (and third parties) store this private information on their servers and/or that Defendants were transmitting this private information to third parties, they would not have purchased Defendants' Smart TVs.

CLASS ACTION ALLEGATIONS

106. Plaintiff brings this action as a class action on behalf of himself and the Class consisting of:

> ***All persons and entities in the United States who, from January 1, 2012 through the present (the "Class Period"), who purchased or leased any LG Smart TVs and/or Sony Smart TVs and/or Samsung Smart TVs that used or contained Automatic Content Software (as defined herein) ("the "Class").***

107. The Class satisfies the numerosity, commonality, typicality, adequacy, predominance and superiority requirements of Federal Rule of Civil Procedure 23(a).

108. Plaintiffs reserve the right to amend or modify the Class definitions with greater specificity or further division into subclasses or limitation to particular issues after discovery.

109. The members of the Class are so numerous that joinder of all members is impracticable. Although the precise number of Class members is unknown to Plaintiffs at this time and can be determined only by appropriate discovery, it is reasonably estimated that the Class consists of at least tens of thousands, or hundreds of thousands, or millions of members who are geographically dispersed throughout the country.

110. Because Plaintiffs are purchasers of Defendants products and have been subject to Defendants' systematic, deceptive and misleading course of conduct,

policies, and advertising intended to trick, mislead and significantly confuse consumers, Plaintiffs are members of the Class and their claims are typical of the claims of the other members of the Class. The harm suffered by Plaintiffs and all other Class members was and is caused by the same misconduct by Defendants.

111. Plaintiffs will fairly and adequately represent and protect the interests of the Class, in that Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel, experienced in consumer and commercial class action litigation, to further ensure such protection and who intend to prosecute this action vigorously.

112. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered by individual Class members are relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims was not available, Defendants would likely continue their wrongful conduct, would unfairly retain many millions of dollars in improperly obtained revenues, or would otherwise escape liability for their wrongdoing as asserted herein.

113. Common questions of law and fact exist as to all members of the Class which predominate over any questions that may affect individual Class members. Among the questions of law and fact common to the Class include the following:

a. whether Defendants' deceptive tracking and monitoring using automatic tracking software, and misleading statements and omissions, caused consumers to purchase Defendants' products;

b. whether Defendants violated the New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 et seq.;

c. whether Defendants violated the Electronic Communications Privacy Act, 18 U.S.C. § 2511;

d. whether Defendants violated the Video Privacy Protection Act, 18 U.S.C. § 2710;

e. whether Defendants breached the implied duty of good faith and fair dealing;

f. whether Defendants were unjustly enriched; and

g. the appropriate measure of damages, restitution, pre- and post-judgment interest, and/or other relief to which Plaintiff and the Class members are entitled.

114. Common questions of law and fact exist as to all members of the Class. The Class is readily definable, and prosecution of this action as a Class Action will reduce the possibility of repetitious litigation. Information concerning Defendants' products is available from Defendants' books and records. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude its maintenance as a Class Action.

115. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendants in this action. Prosecution as a class action will eliminate the possibility of repetitious litigation.

116. The Class is readily definable. Information concerning Defendants' Defendants is available from many sources, including Defendants' books and records.

117. Defendants have acted and/or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

COUNT I

(Unfair and Deceptive Tracking and Transmission - Violations of the CFA)

118. Plaintiff incorporates by reference each preceding and succeeding paragraph as though fully set forth at length herein.

119. Plaintiff brings this cause of action on behalf of himself and on behalf of all other members of the Class.

120. The CFA, N.J. Stat. Ann. § 56:8-2, prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . .

121. The CFA defines "merchandise" as "any objects, wares, goods commodities, services or anything offered, directly or indirectly to the public for sale." N.J. Stat. Ann. § 56:8-1(c).

122. At all relevant times, Defendants have engaged in the advertisement, offering for sale and sale of merchandise within the meaning of N.J. Stat. Ann. § 56:8-1(c), specifically Defendants' Smart TVs and related services.

123. Defendants use ACS technology to comprehensively collect the sensitive television viewing activity of consumers or households across cable or broadband services, set-top boxes, external streaming devices, DVD players, and over-the-air broadcasts, on a second-by-second basis and store this viewing data indefinitely.

124. Defendants provided this viewing data to third parties, which used it to track and target advertising to individual consumers across devices. Defendants engaged in these practices through a medium that consumers would not expect to be used for tracking, without consumers' consent; namely, consumers' own Smart TVs.

125. As described herein, Defendants' continued utilization of unlawful and unconscionable marketing practices, and their continuing practice of monitoring, tracking, and reporting viewing habits and personally identifiable information to unauthorized third parties, without consent, constitutes a deceptive act or practice in violation of the CFA.

126. Further, such is also an unconscionable commercial practice in violation of the CFA. Each instance of Defendants' unfair tracking constitutes a separate violation under the CFA, N.J. Stat. Ann. § 56:8-2.

127. The disclosure of personal viewing history, spending and watching habits, personal voices, and personally-identifiable information is a material term of the transactions at issue as it is likely to affect a consumer's choice of, or conduct regarding, whether to purchase a product or service. The failure to inform consumers that this personal information would be shared with third parties is materially misleading.

128. Defendants' omission of this information was an act likely to mislead Plaintiff and the Class acting reasonably under the circumstances and constitutes a deceptive trade practice in violation of the CFA.

129. Defendants conduct was deceptive and unconscionable because, among other misconduct described in this Complaint, Defendants monitored, tracked, recorded and transmitted to third parties Plaintiffs' and Class members' personal viewing and spending habits and personally identifiable information without providing clear and conspicuous notice and without consent.

130. Defendants' collection and sharing of confidential sensitive data and voices without consumers' consent has caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves.

131. This is an unfair act or practice, in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

132. Defendants' practice of monitoring, tracking, and transmitting to third parties Plaintiffs' and Class members' personal viewing and spending habits and personally identifiable information and voices without providing clear and conspicuous notice and without consent is also unlawful, deceptive and misleading, and violates the Subscriber Privacy Provision in the Cable Communications Policy Act, the Electronic Communications Privacy Act, the FTC Act, and Video Privacy Protection Act, 18 U.S.C. §§ 2710.[48]

133. Defendants violations of these statutes constitute additional violations by Defendants of the CFA.

COUNT II

(Deceptive Omissions - Violations of the CFA)

134. Plaintiffs incorporate by reference all the foregoing paragraphs.

135. Defendants engaged in deceptive practices as defined under the CFA. Defendants' actions were part of a scheme intended to actively mislead Plaintiffs and the Class into believing that the Smart TVs were of a specific quality, namely that the Smart TVs would not violate their privacy and were not designed to violate consumer's privacy by secretly monitoring and recording consumers' viewing habits, while Defendants did in fact know that their Smart TVs were designed to accomplish precisely this objective.

136. Additionally, Defendants did not disclose that their tracking software was installed and/or used on the Smart TVs because they knew that Plaintiffs and the members of the Class would not likely purchase the Smart TVs if they knew of the tracking software.

[48] See infra.

137. Defendants also made material omissions when speaking to Plaintiffs and Class Members through written materials. As described fully above, Defendants failed to clearly and conspicuously inform consumers that once their Smart TVs were hooked up to the internet through an IP address, Defendants would monitor, track, and transmit personal viewing histories and personally-identifiable information and voices to third parties without Plaintiffs' and Class Members' consent.

138. Defendants failed to clearly and conspicuously inform Plaintiffs that once their Smart TV were hooked up to the internet through an IP address, Defendants would monitor and track their and their family's personal viewing histories and personally-identifiable information, and then transmit that confidential information and voices to third parties without Plaintiffs' consent.

139. Defendants also failed to adequately disclose that the ACS feature of their Smart TVs comprehensively collected and shared consumers' television viewing activity from cable boxes, DVRs, streaming devices, and airwaves, which Defendants then provided on a household-by-household basis to third parties (and then to "second-level" third parties) .

140. Defendants' deceptive acts and practices were capable of deceiving a substantial portion of the purchasing public. In fact, the Defendants knew and intended that Plaintiffs and the Class could not be expected to learn about or discover the existence of the Automatic Content Software on the Defendants' Smart TVs.

141. Through these deliberate omissions, the Defendants deceived the Plaintiffs about the quality of the Defendants Smart TVs and, as such, wrongfully induced Plaintiffs to purchase the Smart TVs.

142. The relationship between Defendants and Plaintiffs and the Class gave rise to the duty to speak because Defendants knew that their Smart TVs would, once connected to the internet, obtain confidential information about consumers,

including viewing histories and personally identifiable information, and transmit that information to third parties without the knowledge or consent of the viewer. Defendants had superior knowledge as to the information withheld, and such information was material.

143. By engaging in the deceptive conduct, Defendants obtained substantial financial benefits by selling information about the Plaintiffs and the Class, including personally identifiable information, to unauthorized third parties.

144. The injuries caused by the Defendants' conduct are not outweighed by any countervailing benefits to consumers or competition, and neither Plaintiff nor the Class could have reasonably avoided the injuries they sustained.

145. Defendants intended that Plaintiffs and the Class would rely upon Defendants' deceptive conduct and not be aware of or understand the necessity to uninstall Defendants' Automatic Content software.

146. The acts complained of herein, and each of them, constitute unfair, unlawful or fraudulent business acts or practices in violation of the CFA. Such acts and practices have not abated and will continue to occur unless enjoined.

147. The unfair, unlawful, or fraudulent business acts or practices set forth above have and continue to injure Plaintiffs, the Class, and the general public and cause the loss of money. These violations have unjustly enriched Defendants at the expense of Plaintiffs and the Class.

148. The unfair, unlawful, or fraudulent business acts or practices at issue in this Complaint and carried out by Defendants took place in the course of trade or commerce.

149. As a direct and proximate result of Defendants' violations of the CFA, Plaintiff and the Class have suffered harm in the form of paying monies to purchase the Smart TV when they would not have otherwise.

150. Defendants' failure to adequately disclose its practice of secretly monitoring and tracking consumers and then and then transmitting that private, sensitive data and information and voices to third parties, and other misconduct by Defendants (described herein), also constitute unconscionable commercial practices in violation of the CFA. Each separate instance of Defendants' failure to adequately disclose its practice of secretly monitoring and tracking consumers and then transmitting that private, sensitive data and information and voices to third parties, and other misconduct by Defendants, constitutes a separate violation under the CFA, N.J. Stat. Ann. § 56:8-2.

COUNT III

(Violations Of The Video Privacy Act, 18 U.S.C. § 2710)

151. Plaintiffs incorporates by reference those paragraphs set out above as if fully set forth herein.

152. Defendants are "video tape service providers" as defined by the Video Privacy Protection Act (hereinafter "VPPA"). Defendants "engage[s] in the business, in or affecting interstate or foreign commerce, of rental, sale or deliver of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4). Specifically, Defendants delivers videos and "similar audio visual materials" to consumers through its internet-connected Smart TVs, as well as through many of the pre-loaded applications available on its Smart TVs.

153. Plaintiffs are considered "consumers" under the VPPA because they are each a "renter, purchaser or subscriber of goods or services from a video tape service provider[.]" 18 U.S.C. § 2710(a)(1). As described above, Plaintiffs and the Class caused to be purchased Smart TVs manufactured, marketed, and distributed by Defendants.

154. Plaintiffs and the members of the Class have watched many movies and television shows on the Defendants' Smart TVs. Upon information and belief, at all

times during the Class Period, Defendants' secretly monitored Plaintiffs' and Class members'' usage of their Smart TVs, collected information on Plaintiffs' and Class members' viewing habits, and performed scans of Plaintiffs' and Class members' home WiFi.

155. Unbeknownst to Plaintiffs and members of the Class, Defendants have disclosed and continue to disclose Plaintiffs' and the Class members' information, including their personally identifying information, to unidentified, unauthorized third parties. Upon information and belief, these third parties include advertisers.

156. Defendants' transmissions of Plaintiffs' and the Class members' personally identifiable information to these third party brokers and advertisers constitutes "knowing[] disclosures" of Plaintiffs' and the Class members' "personally identifiable information" to a person under the VPAA. 18 U.S.C. § 2710(a)(1).

157. Plaintiffs and the Class members did not, at any time, consent to Defendants' collection and disclosure of their personally identifiable information to these third party data brokers and advertisers.

158. Defendants' unlawful disclosures constitute a direct violation of the VPAA. Thus, Plaintiffs' and the Class Members' statutory rights under the VPAA have been violated and they are therefore entitled to the maximum statutory and punitive damages available under the VPAA, 18 U.S.C. § 2710(c).

159. A violation of this statute also constitutes a violation of the CFA.[49]

COUNT IV

(Violations Of The Electronic Communications Privacy Act, 18 U.S.C. § 2511)

160. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

[49] See supra.

161. The Electronic Communications Privacy Act ("ECPA") prohibits the "interception and disclosure of wire, oral, or electronic communications."[50]

162. The statute provides that any person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection," violates the ECPA.

163. The statute's definition of "person" includes "corporations."[51]

164. "Oral communications" include only those face-to-face conversations for which the speakers have a justifiable expectation of privacy.[52]

165. "Wire communications" means "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce." [53]

166. Under a few narrow exemptions, ECPA permits the interception of "oral communications" and "wire communications."[54]

167. No exception permits a company to surreptitiously record private communications in the home.

---

[50] 18 U.S. § 2511(1) (2012). (This part of ECPA was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520 (1964 ed,)(Supp. IV)).
[51] 18 U.S.C. 2510(6).
[52] 18 U.S.C. 2510(2). See also US v. Larios, 593 F.3d 82, 92 (1st Cir. 2010).
[53] 18 U.S.C. 2510(1).
[54] 18 U.S.C. 2511(1).

168. By intercepting and recording private communications in the home, Defendants have violated the ECPA.

169. Defendants, either directly or by aiding, abetting, or conspiring to do so, have intentionally intercepted or procured to be intercepted Plaintiffs' and Class Members' electronic communications without Plaintiffs' or Class Members' knowledge, authorization, or consent in violation of 18 U.S.C. § 2511.

170. Defendants, either directly or by aiding, abetting, or conspiring to do so, have also intentionally used or procured to be used a device to intercept the above referenced electronic communications.

171. Defendants conspired to intercept the content of the programs viewed by Plaintiffs and Class Members on their Smart TVs, as alleged herein.

172. Through the loading and enabling of ACS on Smart TVs, collection of communications, and provision of services to permit the illegal interception of electronic communications as alleged herein, Defendants set out on a course of conduct with the intention of intercepting communications of Plaintiffs.

173. An "electronic communication" is defined in § 2510(12) as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce. This definition includes television programming.

174. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally intercepting, endeavoring to intercept, or procuring another person to intercept or endeavor to intercept Plaintiffs' and Class Members' electronic communications.

175. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally collecting, transmitting, storing and disclosing, or endeavoring to disclose, to any other person, the contents of Plaintiffs' and Class Members' electronic communications, knowing

or having reason to know that the information was obtained through the interception of Plaintiffs' and Class Members' electronic communications.

176. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using or endeavoring to use, the contents of Plaintiffs' and Class Members' electronic communications, knowing or having reason to know that the information was obtained through the interception of Plaintiffs' and Class Members' electronic communications.

177. Neither Plaintiffs nor Class Members authorized or consented to Defendants interception of electronic communications.

178. Section 2520 of the ECPA provides for a private cause of action and allows for declaratory and equitable relief as appropriate, damages, disgorgement of profits, and statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, and reasonable attorney's fees and costs.

COUNT V

(Common Law Fraud)

179. Plaintiffs incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

180. Plaintiffs bring this cause of action on behalf of themselves and on behalf of all other members of the Class.

181. Defendants made material misstatements and omissions concerning the Smart TVs that they sold to Plaintiffs and the Class members.

182. As a result, Plaintiffs and Class members were fraudulently induced to purchase Smart TVs.

183. These misstatements and omissions were made by Defendants with knowledge of their falsity, and with the intent that Plaintiffs and Class members rely upon them.

184. Plaintiffs and Class members reasonably relied on these misstatements and omissions, and suffered damages as a result.

COUNT VI

(Breach of Express Warranty)

185. Plaintiffs incorporate by reference and reassert all previous paragraphs.

186. Plaintiffs bring this cause of action on behalf of themselves and on behalf of all other members of the Class.

187. Defendants expressly warranted, among other things, that they would properly and adequately protect Plaintiffs' and the Class members' private data and personal information.

188. Defendants' warranties constitute an affirmation of fact that became part of the basis of the bargain and created an express warranty that Defendants' Smart TV would and could conform to the stated promises.

189. All conditions precedent to Defendants' liability under this contract have been performed by Plaintiffs and the Class.

190. Defendants' breached the terms of this contract, including the express warranties, with Plaintiffs and the Class, by not providing a product that conformed or could possibly conform to Defendants' stated promises of adequately protecting consumers' private information and data, as advertised by Defendants.

191. As a result of Defendants' breach of its contract, Plaintiffs and the Class have been damaged in the amount of the price of the Smart TV products they purchased.

COUNT VII

(Breach of the Duty of Good Faith and Fair Dealing)

192. Plaintiffs incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

193. Plaintiffs bring this cause of action on behalf of themselves and on behalf of all other members of the Class.

194. Every contract in New Jersey contains an implied covenant of good faith and fair dealing.

195. Defendants breached the covenant of good faith and fair dealing by secretly monitoring and tracking Plaintiffs and the members of the Class and transmitting their private, confidential data to third parties, as described herein.

196. Defendants acted in bad faith and/or with a malicious motive to secretly monitor and track Plaintiffs and Class members using ACS, and also acted in bad faith and/or with a malicious motive by transmitting Plaintiffs' and the Class members' private, confidential data to third parties, for profit, thereby causing Plaintiffs and the Class members injuries in an amount to be determined at trial.

COUNT VIII

(Unjust Enrichment)

197. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

198. A measurable benefit has been conferred on Defendants under such circumstances that Defendants' retention of the benefit without payment to Plaintiffs and Class Members would be unjust.

199. The benefit is the taking of Plaintiffs' and Class Members' private Information and capitalizing on it by selling it to third parties for Defendants' monetary gain.

200. The benefit is measurable because Defendants' systematically, through carefully designed computer programs and calculations, commoditized and packaged Plaintiffs' and Class Members' private information and sold it to third parties.

201. Defendants retained both the private information and profits from its

sale.

202. Defendants' retention of the benefits would be unjust because this information was private and personal, it contained personally identifiable information, and Plaintiffs and Class Members would not have voluntarily provided that information for free.

COUNT IX

(Breach of Contract)

203. Plaintiffs incorporate by reference those paragraphs set out above as if fully set forth herein.

204. To the extent that any words transmitted to Plaintiffs and the Class are to be construed in any way to form a contract, such contract would be deemed a classic Contract of Adhesion under common law, without informed consent, and thus unenforceable as a matter of law.

205. Defendants' have thus breached as a matter of law any words transmitted to Plaintiffs and the Class that are construed in any way to form a valid contract.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, prays for relief as follows:

A. For an order that this action may be maintained as a Class Action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs be appointed Class representatives for the Class, and that Plaintiffs' counsel be appointed as counsel for the Class;

B. For a permanent injunction against Defendants, and each of them, restraining, preventing and enjoining Defendants from engaging in the illegal practices alleged;

C. For an order requiring Defendants to halt their practice of secretly and automatically tracking consumers;

D. For an order requiring Defendants to halt their practice of secretly transmitting consumers' private, sensitive information to third-parties;

E. For an order requiring Defendants, and each of them, to disgorge the profits they wrongfully obtained through the use of their illegal practices;

F. For an order requiring Defendants, and each of them, to pay restitution to Plaintiff and all members of the Class.

G. Actual damages;

H. Punitive damages;

I. For an award of attorneys' fees;

J. For an award of the costs of suit incurred herein, including expert witness fees;

K. For an award of interest, including prejudgment interest, at the legal rate, and;

L. For such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury of all claims so triable.

DATED: January 3, 2018 Respectfully submitted,

By: /s/ Michael E. Berman

Michael E. Berman
BERMAN CLASS LAW
1069 Main Street, suite 136
Holbrook, NY 11741
michael@meberman.com